The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/18/2020

SUBJECT:
Multiple Vulnerabilities in SolarWinds N-Central Could Allow for Remote Code Execution

OVERVIEW:
Multiple Vulnerabilities have been discovered in SolarWinds N-Central. Two of these vulnerabilities, when used in conjunction with each other, could allow for remote code execution. SolarWinds N-Central is a remote monitoring and management automation platform for MSPs and IT professionals. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- SolarWinds N-Central Platform version 12.3 HF4

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in SolarWinds N-Central, two of which could allow for remote code execution when used in conjunction. Details of these vulnerabilities are as follows:

- An OS command-injection vulnerability due to traversal issue (CVE-2020-25617). Can be used in conjunction with CVE-2020-25622 for a one-click root RCE attack chain
- A local privilege escalation vulnerability (CVE-2020-25618).
- An unauthorized access vulnerability due to built-in support and admin accounts with default credentials (CVE-2020-25620).
- An unauthorized access vulnerability due to an authentication mechanism in the local Postgres database (CVE-2020-25621).
- A CSRF vulnerability in N-Central Admin Console (CVE-2020-25622). Can be used in conjunction with CVE-2020-25617 for a one-click root RCE attack chain

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions be taken:

- Apply appropriate updates provided by SolarWinds to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privilege user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users no to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

SolarWinds:

https://documentation.solarwindsmsp.com/N-central/Rel_2020-1-2_HF2/N-central_2020-1-2_HF2_ReleaseNotes_en.pdf

Insinuator:

https://insinuator.net/2020/12/security-advisories-for-solarwinds-n-central/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25622